**IDRAC 7,8,9 Configuration Guide**

This document is designed to be used in conjunction with a PUA implementation.

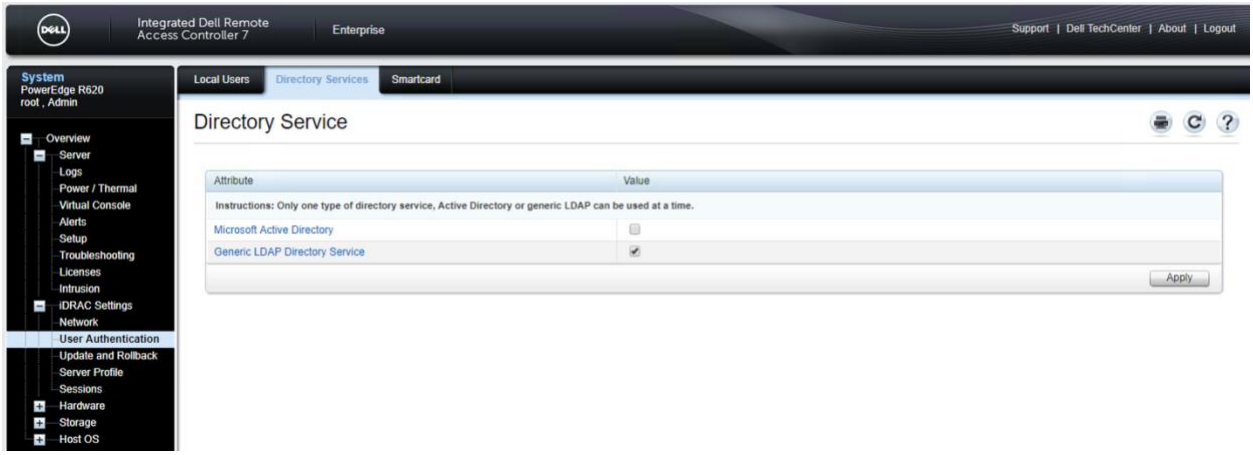
**N.B. It should be noted that this configuration relies on creating a separate VIP and access policy for iDrac and using "Multiple Domain Based SSO" with the login page for this VIP being the main PUA webtop access VIP. Then an "external webtop Item" is created and hosted on the webtop. Also there is an accompanying iRule that injects java script into the login page to force the login. Also note that this configuration is for the HTML5 client for iDrac.**

1) Configure Directory Services for iDrac.

In the case of PUA. iDrac User Interface Must be point "back" to an LDAP VIP on the PUA system for Authentication.

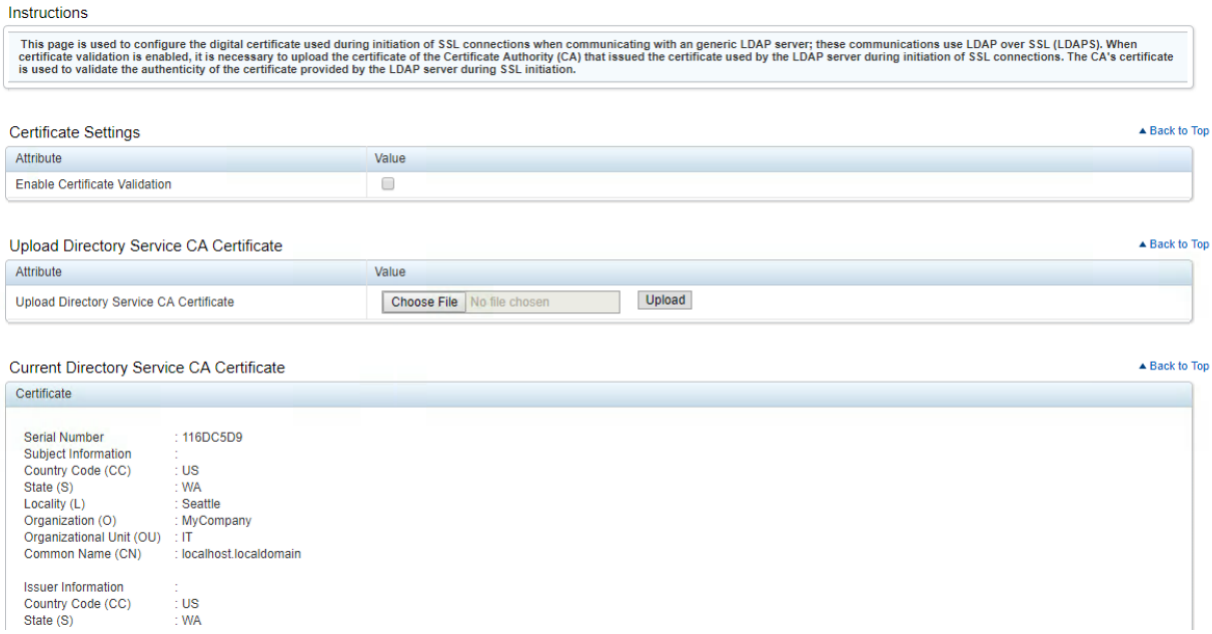
Select System/User Authentication/Directory Services

Click on "Generic LDAP Directory Service"




Select the "Configure Generic LDAP" button..

Upload the Directory Service CA Certificate – in this case the generic F5 self-signed CA Certificate was selected as this was CA Certificate that was associated with the "636" or LDAPS VIP.




Step2 of 3

These are the settings that worked in our case.. depending up on the ultimate Directory these setting may be different. Our “ultimate” back end directory was a Windows Directory.

Enable Generic LDAP “checked”
Use Distinguished Name
LDAP Server Address:- IP of LDAPS VIP for PUA
LDAP Server PORT:- 636.. could be configured to be a different port if the VIP was listening on something other than default.
Bind DN: Whatever you BIND DN would be for your directory… in our case it was cn=Administrator,cn=Users,dc=afspc,dc=local
Attribute of User Login :- sAMAccountName
Attribute of Group Membership:- member

Step 2 of 3

Instructions

This page is used to configure location information about generic LDAP servers and user accounts.

Common Settings ▲ Back to To

| Attribute | Value |
|---|---|
| Enable Generic LDAP | ☑ |
| Use Distinguished Name to Search Group Membership *( if unchecked, username will be used )* | ☑ |
| LDAP Server Address *( FQDN or IP, must match the server certificate if certificate validation is enabled )* | 10.246.49.218 |
| LDAP Server Port *( Only SSL port is supported )* | 636 |
| Bind DN *( required if anonymous bind is not allowed )* | cn=Administrator,cn=Users,dc=afspc,dc=local |
| Update Bind Password | ☐ |
| Bind Password *( required if anonymous bind is not allowed )* | |
| Base DN to Search *( e.g. dc=example,dc=com, required )* | cn=Users,dc=afspc,dc=local |
| Attribute of User Login *( e.g. uid )* | sAMAccountName |
| Attribute of Group Membership *( e.g. member or uniquemember )* | member |
| Search Filter *( e.g. objectclass=*, optional )* | |

Create a Role Group.

Your configuration may be different but each role group will have a role within the iDrac which will have certain group privileges associated with it.

In our case we create a single “Administrator” role group that was associated with a specific group in the Windows Active Directory Server

Step 3a of 3

Instructions

This page is used to configure the privilege groups used to authorize users. When Generic LDAP is enabled, it is necessary to configure Role Group(s) used that specify authorization policy for iDRAC users.

Group Settings ▲ Back to Top

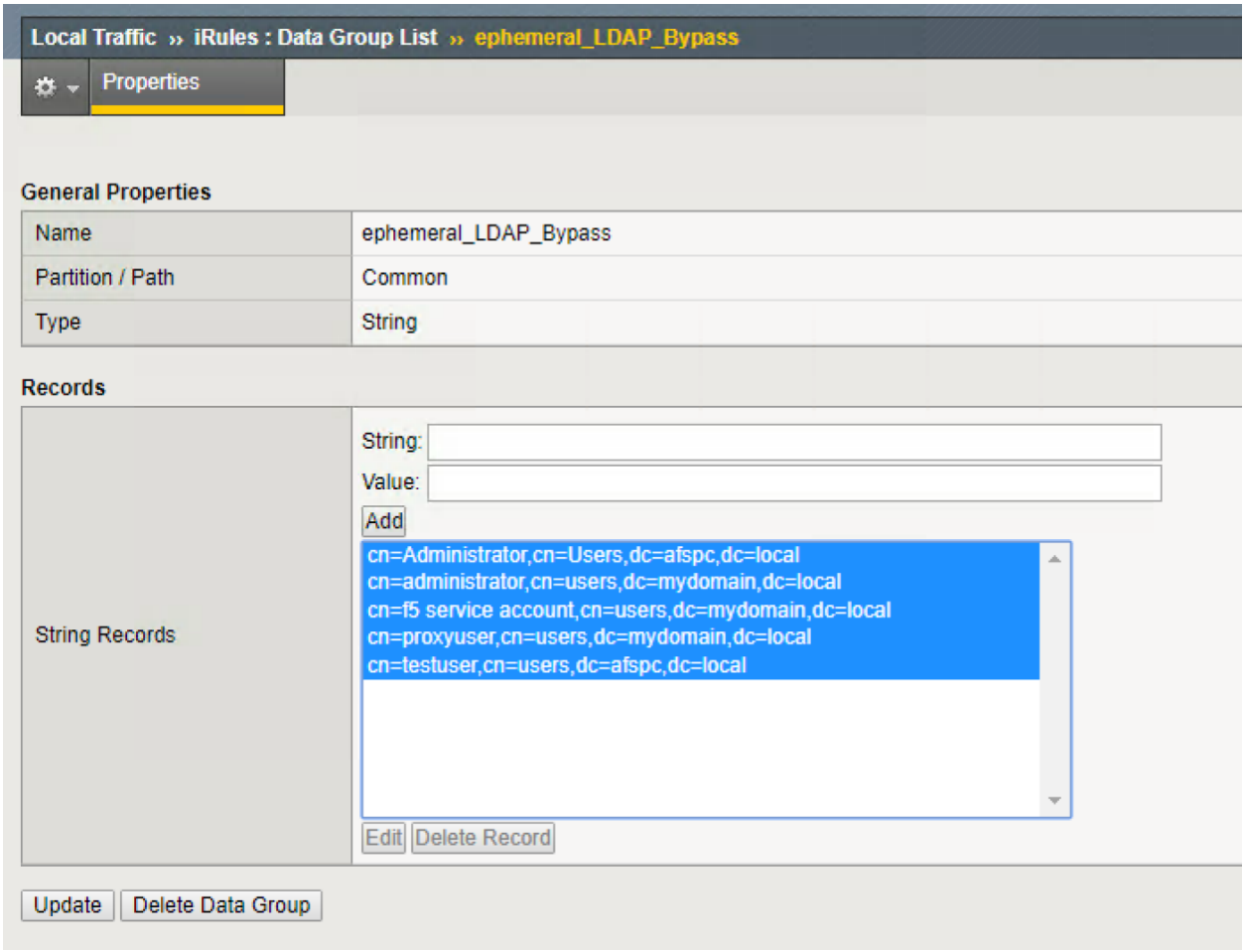
| Role Groups | Group DN | Group Privilege |
|---|---|---|
| Role Group 1 | CN=Administrators,CN=Builtin,DC=afspc,DC=local | Administrator |
| Role Group 2 | | None |
| Role Group 3 | | None |
| Role Group 4 | | None |
| Role Group 5 | | None |

Click Finish..

Select the “Test Settings Button”

Then enter a username and password of an active directory user. If the test passes then you can continue with the F5 Configuration.

**Note: The** DN that username translates to must be in the ephemeral_LDAP_Bypass data-group. Otherwise the PUA system will intercept the authentication and generate an ephemeral credential and the authentication will fail. This data group is under iRules/DataGroup List

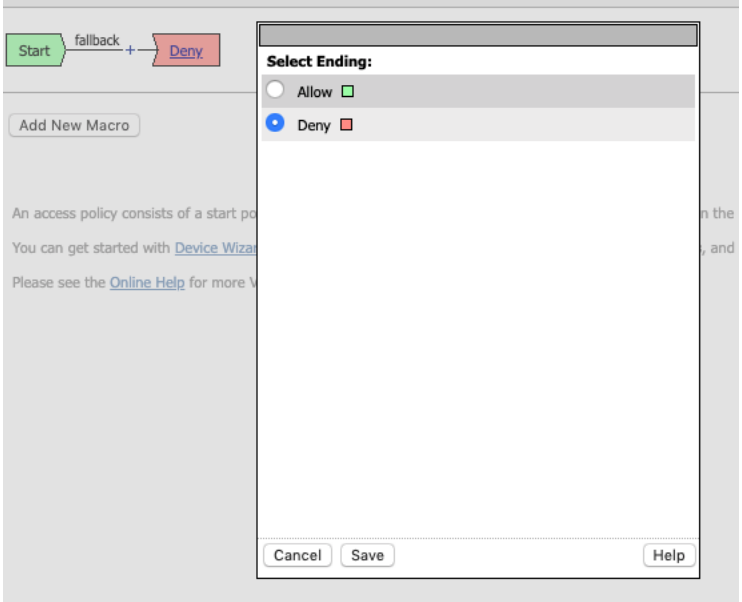



2) Create Access Policy for iDrac

Under Access/ “Profiles/Policies”/Access Profiles (Per Session Policies) click “create”.

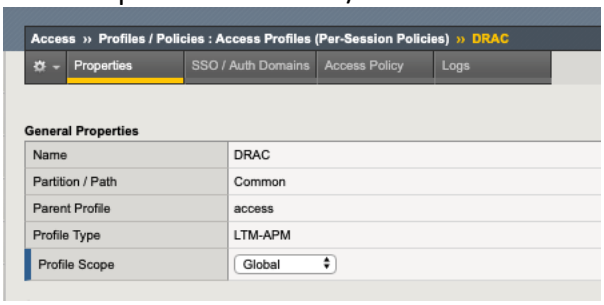
Provide a name for your access Policy for example:- “IDRAC”
For Profile Type Select:- LTM+APM
For Profile Scope Select:- Global
Under Accepted Languages Select:- English
Select Finished.
Under Per Session Policy Select “Edit”

Change the ending to “Allow”.. by clicking on the “Deny” ending and then select the radio button for “Allow”

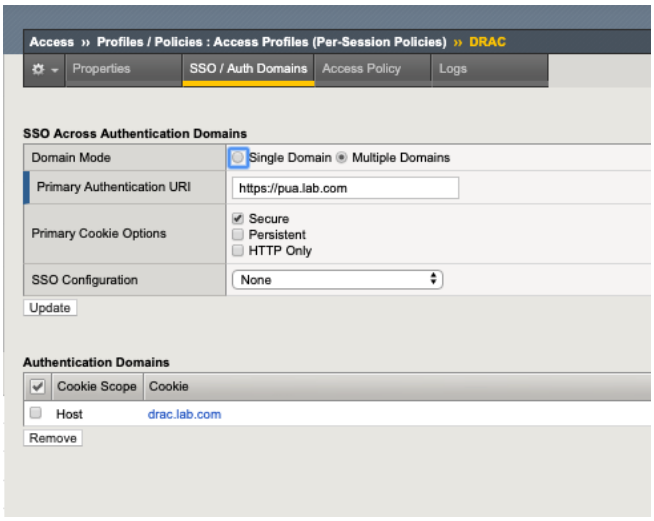



Associate the SSO/Auth Domain with the Access Policy

- Under Access/Profiles/Policies click on the Access Profile Name ..for instance click on “IDRAC” if your access profile is called IDRAC.
- The properties will be displayed..
- At the top click on the SSO/Auth Domains TAB.




- For Domain Mode select “Multiple Domains:
- For primary Authentication URI.. this will be the FQDN for your PUA webtop for instance : https://pua.lab.com
- Under Authentication Domains Select : “Add”
- Then under “Cookie” select “Host”
- For DNS name select the FQDN of the IDrac VIP.
- Make the Cookie “Secure”
- For SSO Configuration select “None”

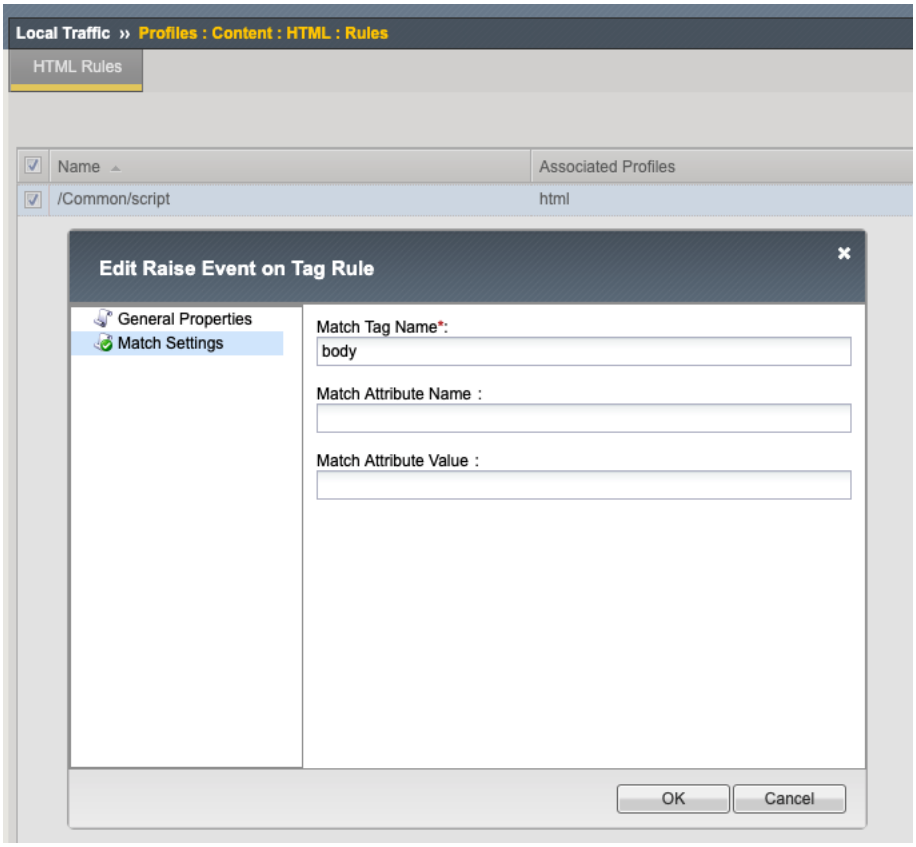



3) Create an HTML content profile rule

This profile will be used in conjunction with the iRule for SSO for IDRAC.

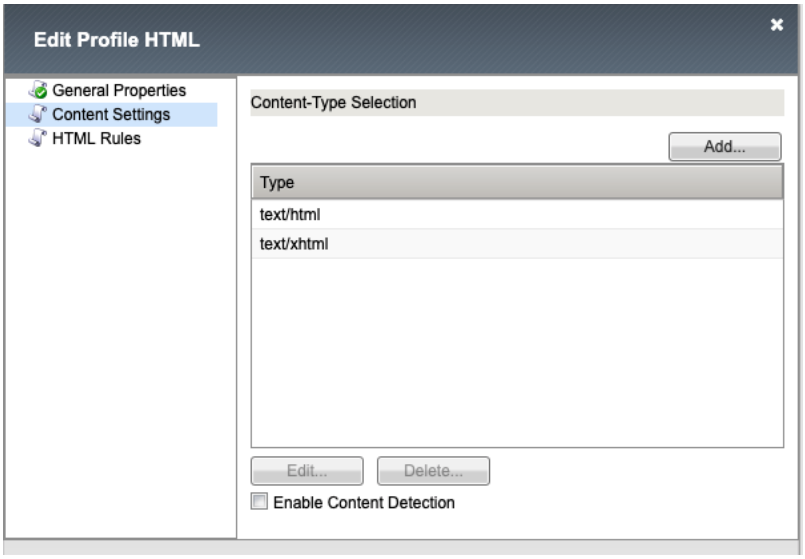
Under Local Traffic/Profiles/Content/HTML/Rules

Select “Create New”
Provide a name:- “Script”
Under “Match Settings” for Match Tag Name type:- body

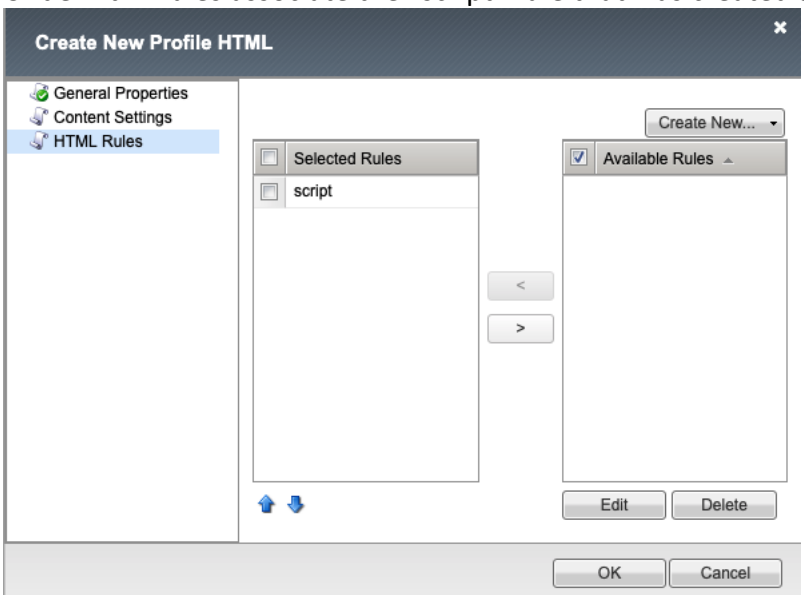



Under.Local Traffic/Profiles/Content/HTML

Select Create Profile
Provide a Profile Name
Under Cotent Settings… add a “Content Type Selection” of
“text/html” and
“text/xhtml”




Under html rules associate the “script” rule that was created above.

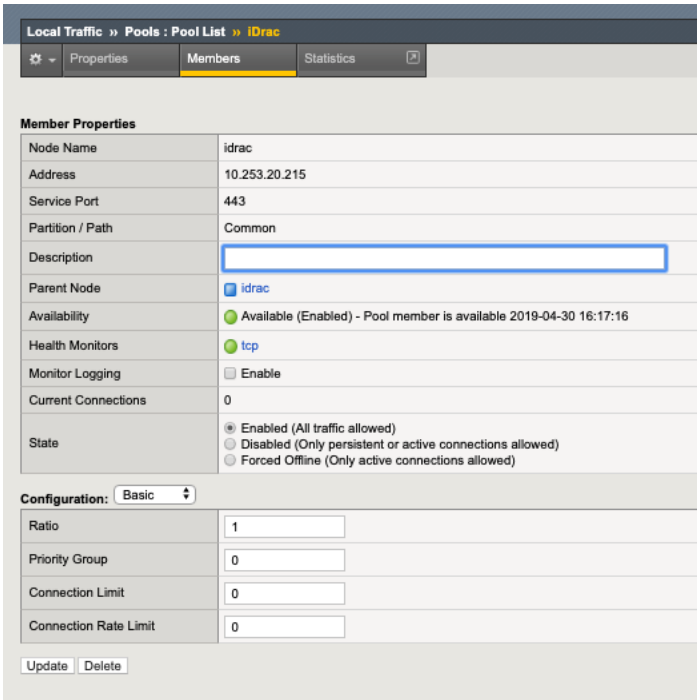



4) Create a pool for IDrac.

N.B. The pool will be associated with the virtual server for IDRAC

Under Local Traffic/Pools/Pool List click “Create”
Provide a Name for the Pool
Select a monitor.
Add the IDrac front end ip as a node to the pool member – make the service port 443 for SSL/TLS.

Click “Finished”




N.B. At this point check that the pool is marked “Available.. “ .. a green circle this will be an indication that the monitor is succeeding and able to make a connection.. the connection type will depend upon the monitor selected.

5) Add the IDrac iRule.

# Needs an HTML profile and an HTML rule looking for tag "body"
#
# ltm profile html html { app-service none content-selection { text/html text/xhtml } rules { script } }
# ltm html-rule tag-raise-event script { match { tag-name body } }
# ltm virtual iDRAC-ext { destination 172.16.1.12:https ip-protocol tcp mask 255.255.255.255 pool iDrac profiles { DRAC { } html { } http { } pua_webtop-clientssl { context clientside } rba { } serverssl { context serverside } tcp { } websso { } } rules { iDracRule } source 0.0.0.0/0 source-address-translation { type automap } translate-address enabled translate-port enabled vs-index 13 }

```
when HTTP_REQUEST {
  HTML::disable
  if { [HTTP::uri] ends_with "/login.html" } {
  HTML::enable
```

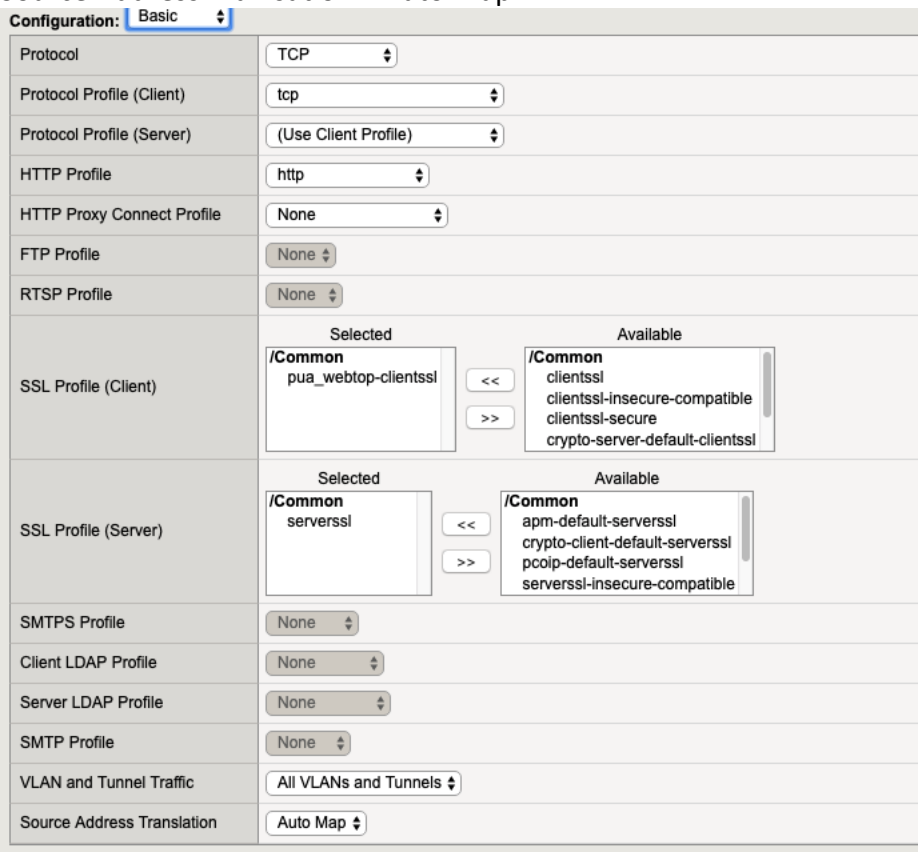
```
  log local0. "HIT LOGIN"
  set workaround 1
  } elseif { [info exists workaround] } {
  unset workaround
  }
}

when HTML_TAG_MATCHED {
  log local0. "at HTML_TAG_MATCHED: [HTML::tag name]"
  if { [info exists workaround] } {
    switch [HTML::tag name] {
      "body" {
        log local0. "at body..."
        set username [ACCESS::session data get session.logon.last.username]
        set password [ACCESS::session data get session.custom.ephemeral.last.password_sso]
        set newstring "<script>
    //Try this
    document.addEventListener('DOMContentLoaded', (event) => {
    console.log('DOM fully loaded and parsed');
    });

    // F5 Patch
    var checkExist = setInterval(function() {
      if (document.body.contains(document.getElementById(\"user\"))) {
        clearInterval(checkExist);
        document.getElementById(\"user\").value = \"$username\";
        document.getElementById(\"password\").value = \"$password\";
        frmSubmit();
      }
    }, 6000); // check every 2000ms

    </script>"
        HTML::tag append $newstring
        unset workaround
        HTML::disable
      }
    }
  }
}
```

6) Create the IDrac VIP.

Under Local Traffic Manager/Virtual Servers Click “Create”

For Source Address:- Your choice.. for instance 0.0.0.0/0
For Destination Address:- This needs to be an IP address.. on the external VLAN.
Service Port: HTTPS

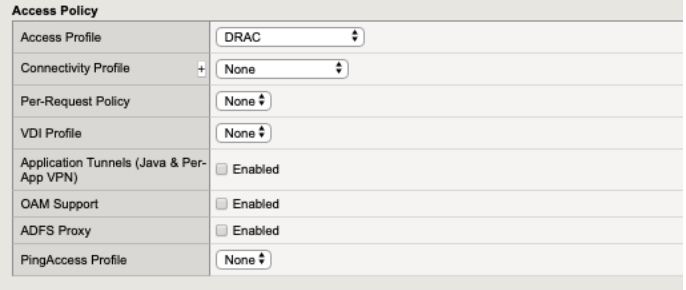
Protocol: TCP
HTTP Profile: http
SSL Profile Client: This needs to be a client SSL profile that is customized for the FQDN for IDrac.
Server SSL: select the “serverssl” profile
Source Address Tranlsation: “Auto Map”



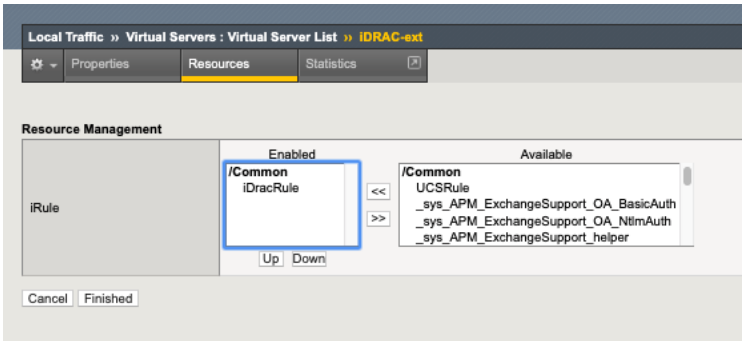

Under Content Rewrite Select “html” (Created Previously)

]

Under Access Policy Select IDrac or whatever you have named your access policy

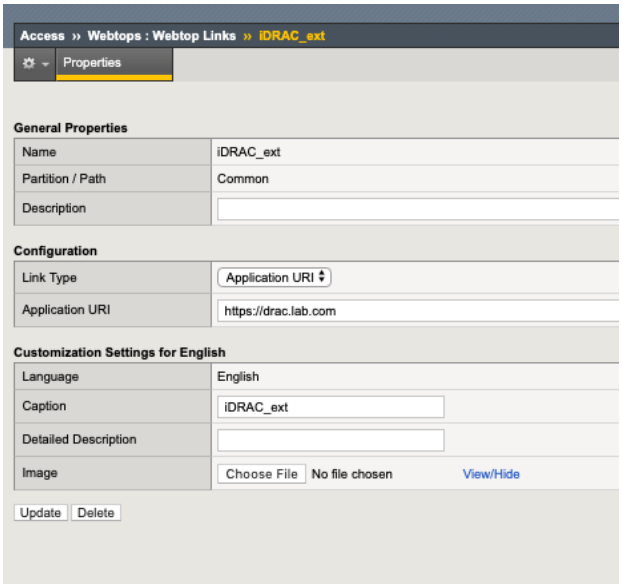



Under Resources
Associate the iDrac iRule that was created previously with the VIP
Associate the pool that was created previously wit the VIP
Select “Finished”




7) Create Portal Access Resource for IDrac

- In the APM menu select Webtops/Webtop Links
  - Click Create
  - Name: Your choice “IDrac” for example
  - Link Type Needs to be Application URI
  - Application URI needs to be the FQDN of the VIP. For example:- https://drac.lab.com
  - For caption: This will be the name that appears on the webtop.




8) You can then associate the IDrac webtop link with the Webtop Policy.

- Click Access/Profiles
- Click “Edit” under Per-Session Policy
- Select the Webtop. This will be associated with an “Advanced Resource Assign Webtop Item”
- Then Select the Add/Delete Button
- Then select the Webtop Links Tab
- Then Select the IDrac webtop link that was created previously.